CLAIMS

What is claimed is:

1. A method of scanning a requested file for a computer malware comprising the steps of:

receiving a request to transfer a file from computer malware scanning software;

receiving a request from the computer malware scanning software for data comprising a randomly accessed portion of the requested file; and

transferring the requested portion of the file and supplying the requested data to the computer malware scanning software to fulfill the request for data comprising a portion of the requested file.

2. The method of claim 1, wherein the request to transfer the file from the computer malware scanning software comprises a request to transfer the file from an external system.

3. The method of claim 2, wherein the external system is communicatively connected via a network.

4. The method of claim 3, wherein the network comprises the Internet.

5. The method of claim 4, wherein the step of transferring the requested portion of the file comprises the step of:

initiating a session with the external system to obtain the requested portion of the file.

6. The method of claim 5, wherein the session is a hypertext transfer protocol session.

7. The method of claim 6, wherein the hypertext transfer protocol session uses a byte range technique.

8. The method of claim 7, further comprising the steps of:

determining that the requested portion of the requested file cannot be transferred; and

transferring the entire requested file and supplying the requested data to the computer malware scanning software to fulfill the request for data comprising a portion of the requested file.

9. The method of claim 8, wherein the requested portion of the requested file cannot be transferred because the requested portion of the requested file cannot be randomly accessed.

10. The method of claim 9, wherein an indication that the requested portion of the requested file cannot be randomly accessed comprises an error indication or a transfer of the entire requested file.

11. The method of claim 7, further comprising the steps of:

tracking information associated with each transfer of a requested portion of the file; and

determining that information associated with the file has changed.

12. The method of claim 11, wherein the information associated with the file comprises hypertext transfer protocol entity tags or last modified timestamp information.

13. The method of claim 12, further comprising the step of:

restarting the requests from the computer malware scanning software for data.

14. The method of claim 13, further comprising the step of:

transferring the entire requested file.

15. The method of claim 1, further comprising the step of:

performing the steps of claim 1 in response to a request from a user system for the file.

16. The method of claim 15, further comprising the steps of:

scanning at the computer malware scanning software the data comprising a portion of the requested file to determine if the file includes a computer malware; and

delivering the file to the user system in response to determining that the file does not include a computer malware.

17. The method of claim 16, wherein the step of delivering the file to the user system comprises the steps of:

determining whether the entire file has been transferred;

starting delivery of the file to the user system even if the entire file has not been transferred; and

transferring those portions of the file that have not been transferred and delivering those portions of the file once they have been transferred.

18. The method of claim 17, wherein the step of transferring those portions of the file that have not been transferred comprises the step of:

initiating a session with the external system to obtain those portions of the file that have not been transferred.

19. The method of claim 18, wherein the session is a hypertext transfer protocol session.

20. The method of claim 19, wherein the hypertext transfer protocol session uses a byte range technique.

21. A system of scanning a requested file for a computer malware virus comprising:

a processor operable to execute computer program instructions;

a memory operable to store computer program instructions executable by the processor; and

computer program instructions stored in the memory and executable to perform the steps of:

receiving a request to transfer a file from computer malware scanning software;

receiving a request from the computer malware scanning software for data comprising a randomly accessed portion of the requested file; and

transferring the requested portion of the file and supplying the requested data to the computer malware scanning software to fulfill the request for data comprising a portion of the requested file.

22. The system of claim 21, wherein the request to transfer the file from the computer malware scanning software comprises a request to transfer the file from an external system.

23. The system of claim 22, wherein the external system is communicatively connected via a network.

24. The system of claim 23, wherein the network comprises the Internet.

25. The system of claim 24, wherein the step of transferring the requested portion of the file comprises the step of:

initiating a session with the external system to obtain the requested portion of the file.

26. The system of claim 25, wherein the session is a hypertext transfer protocol session.

27. The system of claim 26, wherein the hypertext transfer protocol session uses a byte range technique.

28. The system of claim 27, further comprising the steps of:

determining that the requested portion of the requested file cannot be transferred; and

transferring the entire requested file and supplying the requested data to the computer malware scanning software to fulfill the request for data comprising a portion of the requested file.

29. The system of claim 28, wherein the requested portion of the requested file cannot be transferred because the requested portion of the requested file cannot be randomly accessed.

30. The system of claim 29, wherein an indication that the requested portion of the requested file cannot be randomly accessed comprises an error indication or a transfer of the entire requested file.

31. The system of claim 27, further comprising the steps of:

tracking information associated with each transfer of a requested portion of the file; and

determining that information associated with the file has changed.

32. The system of claim 31, wherein the information associated with the file comprises hypertext transfer protocol entity tags or last modified timestamp information.

33. The system of claim 32, further comprising the step of:

restarting the requests from the computer malware scanning software for data.

34. The system of claim 33, further comprising the step of:

transferring the entire requested file.

35. The system of claim 21, further comprising the step of:

performing the steps of claim 1 in response to a request from a user system for the file.

36. The system of claim 35, further comprising the steps of:

scanning at the computer malware scanning software the data comprising a portion of the requested file to determine if the file includes a computer malware; and

delivering the file to the user system in response to determining that the file does not include a computer malware.

37. The system of claim 36, wherein the step of delivering the file to the user system comprises the steps of:

determining whether the entire file has been transferred;

starting delivery of the file to the user system even if the entire file has not been transferred; and

transferring those portions of the file that have not been transferred and delivering those portions of the file once they have been transferred.

38. The system of claim 37, wherein the step of transferring those portions of the file that have not been transferred comprises the step of:

initiating a session with the external system to obtain those portions of the file that have not been transferred.

39. The system of claim 38, wherein the session is a hypertext transfer protocol session.

40. The system of claim 39, wherein the hypertext transfer protocol session uses a byte range technique.

41. A computer program product of scanning a requested file for a computer malware comprising:

a computer readable medium;

computer program instructions, recorded on the computer readable medium, executable by a processor, for performing the steps of

receiving a request to transfer a file from computer malware scanning software;

receiving a request from the computer malware scanning software for data comprising a randomly accessed portion of the requested file; and

transferring the requested portion of the file and supplying the requested data to the computer malware scanning software to fulfill the request for data comprising a portion of the requested file.

42. The computer program product of claim 41, wherein the request to transfer the file from the computer malware scanning software comprises a request to transfer the file from an external system.

43. The computer program product of claim 42, wherein the external system is communicatively connected via a network.

44. The computer program product of claim 43, wherein the network comprises the Internet.

45. The computer program product of claim 44, wherein the step of transferring the requested portion of the file comprises the step of:

initiating a session with the external system to obtain the requested portion of the file.

46. The computer program product of claim 45, wherein the session is a hypertext transfer protocol session.

47. The computer program product of claim 46, wherein the hypertext transfer protocol session uses a byte range technique.

48. The computer program product of claim 47, further comprising the steps of:

determining that the requested portion of the requested file cannot be transferred; and

transferring the entire requested file and supplying the requested data to the computer malware scanning software to fulfill the request for data comprising a portion of the requested file.

49. The computer program product of claim 48, wherein the requested portion of the requested file cannot be transferred because the requested portion of the requested file cannot be randomly accessed.

50. The computer program product of claim 49, wherein an indication that the requested portion of the requested file cannot be randomly accessed comprises an error indication or a transfer of the entire requested file.

51. The computer program product of claim 47, further comprising the steps of:

tracking information associated with each transfer of a requested portion of the file; and

determining that information associated with the file has changed.

52. The computer program product of claim 51, wherein the information associated with the file comprises hypertext transfer protocol entity tags or last modified timestamp information.

53. The computer program product of claim 52, further comprising the step of:

restarting the requests from the computer malware scanning software for data.

54. The computer program product of claim 53, further comprising the step of:

transferring the entire requested file.

55. The computer program product of claim 41, further comprising the step of:

performing the steps of claim 1 in response to a request from a user system for the file.

56. The computer program product of claim 55, further comprising the steps of:

scanning at the computer malware scanning software the data comprising a portion of the requested file to determine if the file includes a computer malware; and

delivering the file to the user system in response to determining that the file does not include a computer malware.

57. The computer program product of claim 56, wherein the step of delivering the file to the user system comprises the steps of:

determining whether the entire file has been transferred;

starting delivery of the file to the user system even if the entire file has not been transferred; and

transferring those portions of the file that have not been transferred and delivering those portions of the file once they have been transferred.

58. The computer program product of claim 57, wherein the step of transferring those portions of the file that have not been transferred comprises the step of:

initiating a session with the external system to obtain those portions of the file that have not been transferred.

59. The computer program product of claim 58, wherein the session is a hypertext transfer protocol session.

60. The computer program product of claim 59, wherein the hypertext transfer protocol session uses a byte range technique.